(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication : **0 666 671 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt : **95400161.6**

(51) Int. Cl.[6] : **H04L 29/06**

(22) Date de dépôt : **25.01.95**

(30) Priorité : **01.02.94 FR 9401091**

(43) Date de publication de la demande :
09.08.95 Bulletin 95/32

(84) Etats contractants désignés :
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Demandeur : **DASSAULT AUTOMATISMES ET TELECOMMUNICATIONS**
9, rue Elsa Triolet
Z.I. Les Gatines,
B.P.13
F-78373 Plaisir Cédex (FR)

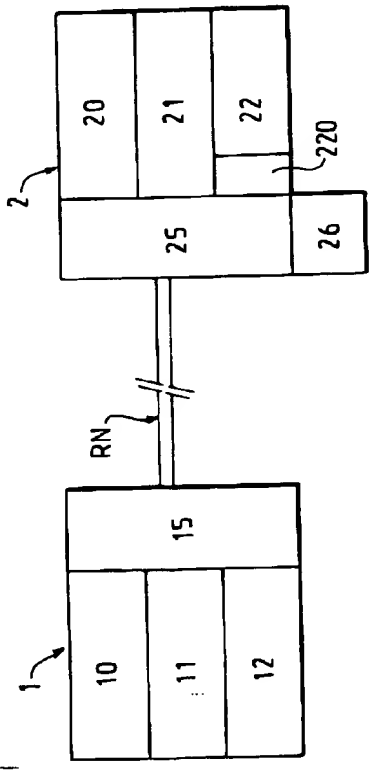
(72) Inventeur : **Basset, Jean-Claude**
84, rue Vergniaud
F-75013 Paris (FR)

(74) Mandataire : **Plaçais, Jean-Yves**
Cabinet Netter,
40, rue Vignon
F-75009 Paris (FR)

(54) Communication sur réseau numérique, avec anti-virus.

(57) Un poste (1) émet, grâce à une interface de communication (15) et selon un protocole déterminé, des données de fichier, en direction de l'interface de communication (25) d'un poste récepteur (2). Ce poste récepteur (2) stocke temporairement les données émises par le poste émetteur (1) dans une mémoire spécifique (26) qui les soumet à un module chercheur anti-virus (220), avant qu'il ne les transforme en données utilisables par une unité de traitement (22), si la recherche anti-virus est négative.

FIG.2



EP 0 666 671 A1

L'invention concerne les réseaux de communication informatiques étendus, en particulier publics.

De façon générale, ces réseaux transmettent des informations ou données brutes. Mais on tend maintenant à les utiliser pour transmettre aussi des fichiers, qui sont un ensemble de données organisées.

En France par exemple, la Société FRANCE TÉLÉCOM a maintenant normalisé un protocole de transfert de fichiers dit STUDEL, et développé une application correspondante de transfert de fichiers dénommée TÉLÉDISQUETTE. Ce système de transfert de fichiers utilise le réseau numérique à intégration de services ou RNIS, commercialisé sous la Marque NUMÉRIS.

Le passage à des transferts de fichiers directement utilisables dans un micro-ordinateur présente de nombreux avantages. Tout d'abord le mode de mise en relation des utilisateurs, ainsi que les moyens logiciels de transfert, peuvent être standardisés, ce qui les rend multi-constructeurs et multi-utilisateurs. En outre, ce système peut être assorti d'un annuaire recensant les récepteurs à ce service, et aussi offrir des fonctions de diffusion automatique. En bref, on peut ainsi envisager une technique de transfert de fichiers par le réseau public, qui possède pratiquement les mêmes caractéristiques de convivialité que la téléphonie vocale actuelle.

Il reste qu'un tel système est vulnérable à la transmission de fichiers qui incluraient un agent intrus et/ou nocif, tel qu'un virus informatique.

La présente invention vient apporter une solution à ce problème.

Elle part d'un dispositif de communication informatique, qui comprend :

- au moins un poste émetteur muni d'une unité de traitement avec une mémoire de travail, une mémoire de masse, et une interface de communication,
- au moins un poste récepteur muni d'une unité de traitement avec une mémoire de travail, une mémoire de masse, et une interface de communication,
- les deux interfaces de communication étant aptes à dialoguer à travers un réseau numérique d'accès public, et les deux postes étant munis de modules de communication respectifs d'émetteur et de récepteur conformes à un protocole prédéterminé, propre au transfert de fichiers.

Selon l'invention, le poste récepteur comporte une partie de mémoire spécifique, éligible comme inapte en général aux échanges avec son unité de traitement, sauf éventuellement pour le module de communication de récepteur, ainsi qu'un module chercheur anti-virus ; le module de communication stocke les données de fichier incidentes dans ladite partie de mémoire de masse spécifique ; il les soumet au module chercheur anti-virus avant de les transformer en un fichier utilisable et de les rendre accessibles d'une manière générale à l'unité de traitement.

Le module anti-virus peut opérer sur les données de fichier reçues en série pendant leur réception. Il peut également opérer sur le regroupement des données du fichier, par exemple dans un fichier temporaire, avant leur transformation en fichier utilisable.

Bien entendu les rôles des émetteurs et des récepteurs ne sont pas figés comme indiqué, et on peut imaginer qu'un émetteur soit également récepteur, et réciproquement.

Plus généralement, le module de communication d'émetteur peut être muni de moyens anti-virus comme celui d'un récepteur.

On peut encore prévoir un mode spécial, par lequel le module récepteur est propre à substituer au module anti-virus en cours une version mise à jour de celui-ci, reçue de l'émetteur, après contrôle de la version mise à jour par la version précédente disponible.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et des dessins annexés, sur lesquels :

- la figure 1 illustre de façon générale des émetteurs et des récepteurs interconnectés par le réseau numérique public ;
- la figure 2 est un schéma de principe restreint à un poste émetteur et un poste récepteur ; et
- les figures 3 et 4 sont deux schémas partiels détaillés illustrant deux variantes de mise en oeuvre de la présente invention.

Sur la figure 1, la référence RN désigne un réseau numérique étendu, ou public, comme le réseau numérique à intégration de services connu en France sous la dénomination "Numéris".

A ce réseau peuvent être connectés des émetteurs SV1 et SV2, ainsi que des récepteurs AB1 à AB4.

Les postes émetteurs et récepteurs sont par exemple (non limitatif) agencés à la manière d'installations micro-informatiques.

Ainsi, sur la figure 2, l'émetteur 1 comporte une unité de traitement 10 avec une mémoire de travail 11 et une mémoire de masse 12, ainsi qu'une interface de communication 15, qui peut également comporter des fonctions électroniques.

De même, le poste récepteur 2 est muni d'une unité de traitement 20, d'une mémoire de travail 21, d'une mémoire de masse 22 et d'une interface de communication 25 qui peut elle aussi avoir des fonctions intégrées.

Les deux interfaces de communication 15 et 25 sont aptes à dialoguer à travers le réseau numérique RN. Les deux postes sont munis de modules de communication respectifs d'émetteur et de récepteur, opérant par exemple conformément à l'application de transfert TELEDISQUETTE, qui permet le transfert

de fichiers, et s'appuie sur le protocole normalisé STUDEL déjà cité, (également désigné par EUROFILE TRANSFER dans une norme ETS des EUROPEAN TELECOMMUNICATION STANDARD INSTITUTES).

Un système de transfert de fichiers possède en général ses propres dispositifs de sécurité, par code d'accès et authentification par exemple, ce qui nécessite l'accord conjoint de l'émetteur et du récepteur.

Cependant l'ouverture d'un tel service à l'ensemble des utilisateurs implique que certains fichiers pourront être transmis sans l'accord préalable des intéressés, donc sans mise en oeuvre des dispositifs de sécurité internes du système de transfert de fichiers.

Ainsi, un fichier transféré peut se trouver infecté par un virus informatique.

Un virus informatique est une séquence de données introduite dans un logiciel et/ou un fichier, et qui peut déclencher des actions néfastes au fonctionnement normal du système informatique qui l'héberge. On sait qu'un virus peut être par exemple actif, passif ou déclenché.

Parmi les techniques anti-virus connues, on peut mettre à part celles qui se contentent de détecter la présence d'un virus, en remarquant ses effets, après qu'ils se soient produits. Cette détection des virus par leurs effets avérés n'est guère applicable ici: par son principe elle signifie que le virus a déjà pu infecter de nombreux fichiers locaux.

Les techniques les plus performantes repèrent les virus informatiques d'après leur structure, et/ou dès qu'ils commencent à agir. Autant que possible, elles corrigent les effets du virus détecté, le cas échéant. C'est ce qu'on appelle ici un "chercheur de virus".

Mais les virus sont très variés, et leurs créateurs imaginatifs. Des virus nouveaux apparaissent régulièrement. Il est souhaitable de procéder à des mises à jour régulières de l'outil chercheur anti-virus, pour tenir compte de nouvelles structures de virus récemment relevées.

L'application classique de ces chercheurs de virus nécessite de nombreuses manipulations manuelles, à effectuer chaque fois que l'on reçoit de nouveaux fichiers, que ce soit par une disquette, ou d'une autre manière. Il est d'ailleurs préférable de placer sur disquette les fichiers suspects pour les vérifier.

Selon l'invention, le poste récepteur 2 comporte une partie de mémoire spécifique, représentée ici en 26 à côté de l'interface de communication 25.

Par des moyens matériels ou logiciels, cette mémoire spécifique 26 est éligible comme inapte en général aux échanges avec son unité de traitement 20, sauf éventuellement pour le module de communication récepteur 25.

Une façon de faire consiste à munir l'installation informatique d'un second disque dur indépendant, et accessible seulement à l'interface de communication 25, laquelle comporte alors des moyens convenables de gestion d'un tel disque dur.

Une autre façon de procéder consiste, dans les systèmes d'exploitation admettant des privilèges d'accès aux fichiers en lecture et écriture, à faire en sorte qu'une partie de la mémoire de masse 22 soit strictement réservée en lecture et écriture au module de communication 25, au moins lorsque celui-ci est en opération.

Une troisième façon de procéder pourrait consister à réserver simplement l'accès à des fichiers pour l'interface de communication 25, en prenant soin de donner à ces fichiers des caractéristiques telles qu'ils ne puissent être utilisables par l'unité de traitement 20, tout particulièrement comme des fichiers de programmes, que l'on appelle encore fichiers exécutables.

Un module chercheur anti-virus 220 est implanté soit dans la mémoire de masse 22, soit dans la partie de mémoire additionnelle 26, lorsque celle-ci dispose de suffisamment de place.

Le module de communication 25 stocke l'intégralité des données de fichiers incidentes dans la partie de mémoire de masse 26, et il les soumet au module chercheur anti-virus, avant de les transformer en un fichier utilisable, qui soit de surcroît rendu accessible de façon générale (c'est-à-dire sans réserve) à l'unité de traitement 20.

On a indiqué plus haut que la mémoire 26 peut être une mémoire de masse directement accessible à l'interface de communication 25. Sur la figure 3A, cette mémoire est illustrée en 261 sous la forme d'une mémoire ou d'un registre de grande capacité, dont l'adressage et la lecture sont réservés au module anti-virus, illustré en 220A, lequel n'autorise l'accès aux données reçues (ce qui est schématisé par la fermeture d'un interrupteur 28A), que lorsqu'il a pu assurer que les données reçues sont dénuées de tout virus connu.

En d'autres termes, le module anti-virus 220A opère ici sur les données du fichier reçues en série, pendant leur réception.

L'homme du métier saura en effet réaliser à partir de la figure 3A un dispositif à plusieurs sections dans la mémoire 261, qui permette de recevoir en série des données tout en les contrôlant et en les laissant sortir également en série par fermeture convenable de l'interrupteur 28A.

De préférence (au moins pour les fichiers de grande taille), le module anti-virus opère sur le regroupement des données en fichiers. C'est ce qui est illustré sur la figure 3B.

La mémoire de masse 26 est alors un disque dur additionnel 262, où l'on peut stocker par exemple, sous la forme de fichiers temporaires (notés par "TMP"), l'ensemble des données reçues depuis l'émetteur.

Le contrôle peut alors s'effectuer après la réception complète du fichier, par le module anti-virus illustré ici en 220B, et qui comme précédemment possède l'accès d'adressage et de lecture au disque dur 262.

Lorsque son contrôle est terminé, le module 220B autorise l'accès, schématisé par la fermeture de l'interrupteur 28B, à la mémoire de masse principale 22B du poste récepteur 2, où le fichier reçu peut être par exemple transformé en fichier exécutable (ce qui est noté par la marque "EXE").

De façon totalement inconnue du module émetteur, le module récepteur peut ainsi vérifier que tous les fichiers reçus sont dénués de tout virus.

Bien entendu, un contrôle de même nature peut être effectué au niveau du module émetteur.

De plus, on peut utiliser dans le module émetteur exactement la même structure que dans le module récepteur, si le besoin s'en fait sentir, et en particulier si le émetteur peut également jouer le rôle récepteur pour d'autres émetteurs.

Le module anti-virus 220 peut devoir, pour des raisons déjà indiquées, être modifié pour incorporer de nouvelles versions de virus récemment découvertes.

Une variante intéressante de l'invention consiste à transmettre les modules anti-virus depuis un émetteur.

Dans ce cas, le module récepteur recevra un ordre spécial, représentatif d'un mode spécial de travail. Il reçoit le module anti-virus nouveau ou mis à jour comme tout autre fichier. Mais, après vérification de celui-ci par le module anti-virus dont il disposait jusqu'à présent, il va pouvoir remplacer ce dernier par le nouveau module anti-virus, si du moins le contrôle a été négatif.

Bien entendu la présente invention n'est pas limitée au mode de réalisation décrit. Elle s'étend à toute variante que pourra développer l'homme du métier, en particulier dans le cadre des revendications ci-après.

Pour des raisons aisément compréhensibles, la présente description n'entre pas dans le détail des structures connues de virus informatiques, ni des différentes variantes de l'invention qui peuvent en découler.

Ceci étant, le mot "virus informatique" est à prendre ici au sens large, couvrant tout agent, intrus ou ajouté délibérément, susceptible d'avoir une action néfaste ou nocive, même bénigne, sur un système informatique. On sait que l'action néfaste peut simplement consister à occuper inutilement de la place en mémoire vive ou en mémoire de masse. Ainsi, l'invention peut s'appliquer non seulement aux "virus" proprement dits, qui infectent un système informatique en se propageant et se multipliant, parallèlement à leur action nocive (comme les virus biologiques), mais aussi notamment à leurs variantes logicielles comme les "chevaux de Troie", les "bombes", et les "vers".

De telles variantes existent en ce qui concerne le réseau utilisé:

- le service décrit ci-dessus (RNIS/SND-Numéris) opère en mode "circuit", c'est-à-dire relie les deux stations en simulant une connexion directe entre elles;
- l'invention peut aussi s'appliquer aux modes de transmission dits "datagramme" ou par paquets (norme X25), dans lesquels les différents groupes ou paquets de données peuvent passer par des chemins différents. La taille de la mémoire utilisée pour regrouper les données est ajustée en conséquence.

Des variantes existent également en ce qui concerne le rôle des stations:

- dans un mode "à serveur", il existe un nombre limité de stations (les serveurs) qui ont vocation à transmettre des fichiers à des stations ordinaires (les abonnés), dans le cadre de liaisons point-à-point via un réseau public ou étendu. Ceci convient aux organisations qui ont un service centralisé, par exemple pour la télédiffusion, le téléchargement ou la télémaintenance de logiciels.
- dans un autre mode ("à station"), on considère simplement des stations émettrice et réceptrice, ou plus fréquemment émettrices/réceptrices. Ce sont par exemple les abonnés du mode à serveur qui dialoguent directement entre eux pour l'échange de fichiers.

Revendications

1. Dispositif de communication informatique, du type comprenant:
   - au moins un poste émetteur (1) muni d'une unité de traitement (10) avec une mémoire de travail (11), une mémoire de masse (12), et une interface de communication (15),
   - au moins un poste récepteur (2) muni d'une unité de traitement (20) avec une mémoire de travail (21), une mémoire de masse (22), et une interface de communication (25),
   - les deux interfaces de communication (15,25) étant aptes à dialoguer à travers un réseau numérique d'accès (RN), et les deux postes étant munis de modules de communication respectifs d'émetteur et de récepteur conformes à un protocole prédéterminé, propre au transfert de fichiers,

   caractérisé en ce que le poste récepteur (2) comporte une partie de mémoire spécifique (26), éligible comme inapte en général aux échanges avec son unité de traitement, sauf pour le module de communication récepteur, ainsi qu'un module chercheur anti-virus (220), en ce que le module

de communication (25) stocke les données de fichier incidentes dans ladite partie de mémoire de masse (26), et en ce qu'il les soumet au module chercheur anti-virus (220) avant de les transformer en un fichier utilisable et de les rendre accessible d'une manière générale à l'unité de traitement.

2. Dispositif selon la revendication 1, caractérisé en ce que le module anti-virus (220A) opère sur les données de fichier reçues en série, pendant leur réception (261).

3. Dispositif selon l'une des revendications 1 et 2, caractérisé en ce que le module anti-virus (220B) opère sur le regroupement des données de fichier (262), avant leur transformation en fichier utilisable (22B).

4. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le module de communication (15) d'émetteur est muni de moyens anti-virus comme celui d'un récepteur.

5. Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'en un mode spécial, le module récepteur est propre à substituer au module anti-virus en cours une version mise à jour de celui-ci, reçue de l'émetteur, après contrôle de la version mise à jour par la précédente.

6. Dispositif selon l'une des revendications précédentes, caractérisé en ce que ladite partie de mémoire spéciale (26) est une partie de la mémoire de masse, ou une mémoire de masse additionnelle (22B).

7. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le protocole de communication est un protocole normalisé d'usage public.

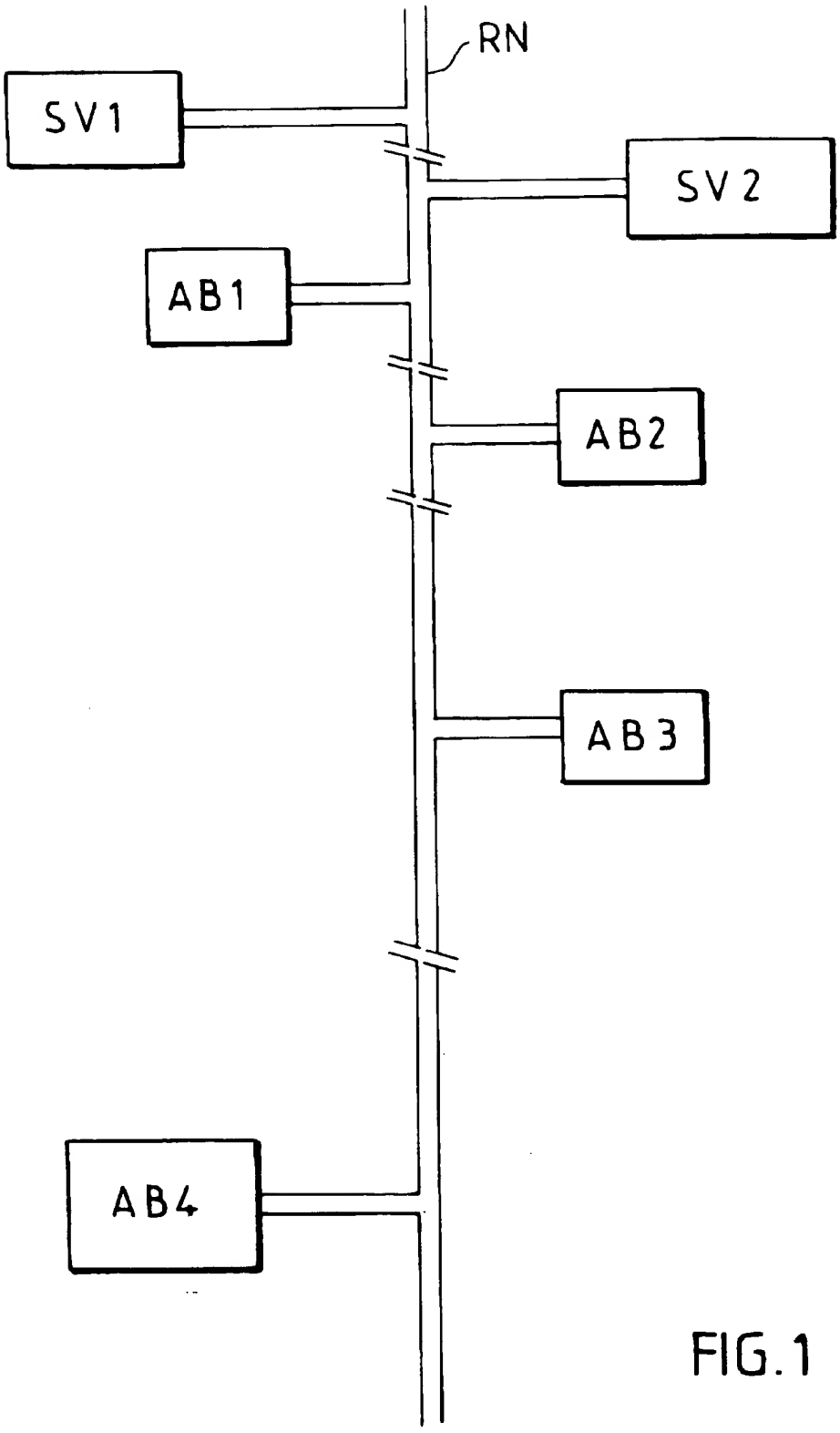


FIG.1

FIG.2

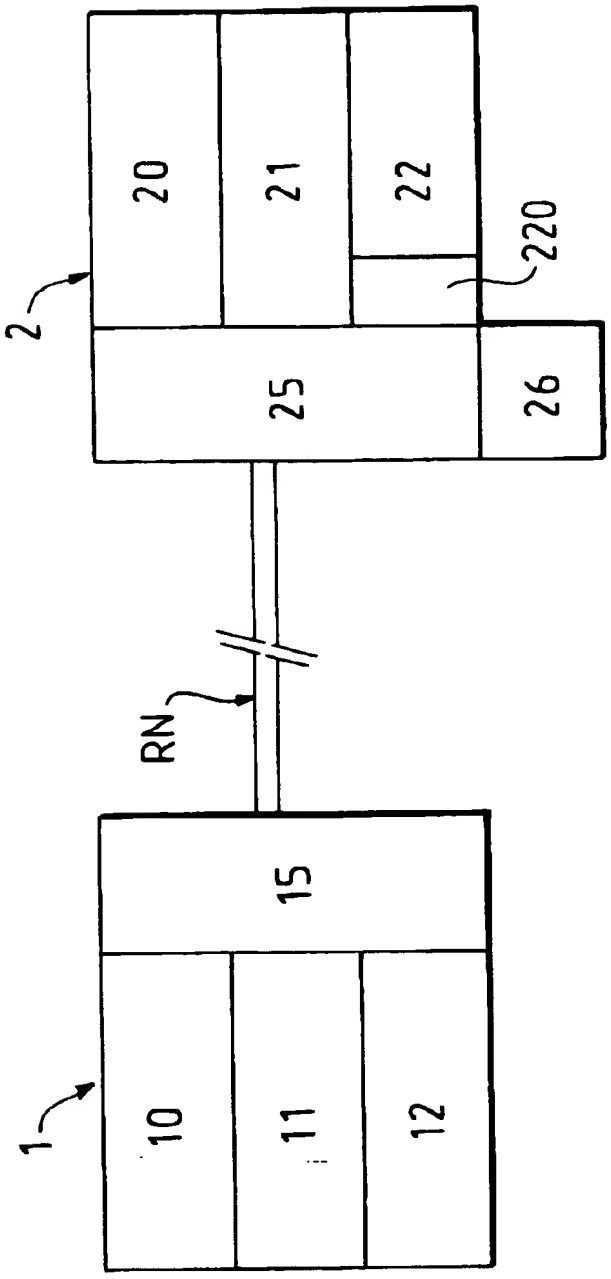


FIG.3B

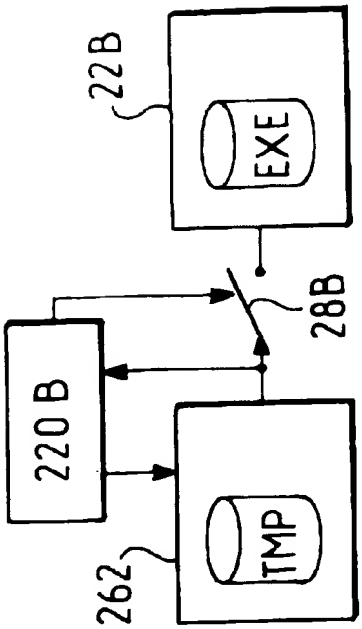
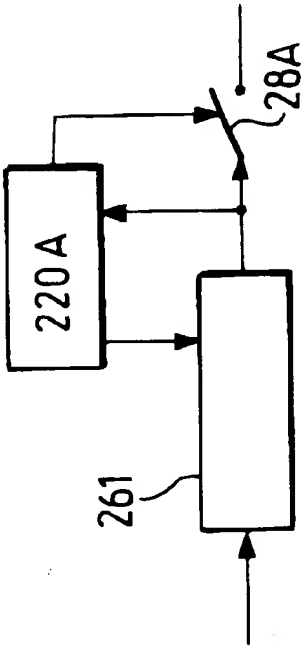


FIG.3A



Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 95 40 0161

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
X	WO-A-93 22723 (MULTI-INFORM A/S) * page 1, ligne 22 - page 3, ligne 2 * * page 4, ligne 1 - page 7, ligne 2 * * figure 1 *	1-3	H04L29/06
A	---	4-7	
A	DATAMATION, vol.37, no.20, Octobre 1991, BARRINGTON US pages 87 - 90 M.SCHLACK 'HOW TO KEEP VIRUSES OFF YOUR LAN' * le document en entier * ---	1-7	
A	COMPUTER NETWORKS AND ISDN SYSTEMS., vol.17, no.2, Juillet 1989, AMSTERDAM NL pages 141 - 148, XP34508 D.M.CHESS 'COMPUTER VIRUSES AND RELATED THREATS TO COMPUTER AND NETWORK INTEGRITY' * alinéa 4 * -----	1-7	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G06F
H04L

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	18 Mai 1995	Canosa Areste, C

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C01)

19 European Patent Office

11 Publication number: 0 666 671 A1

12 **EUROPEAN PATENT APPLICATION**

21 Appl. No.: 95400161.1

51 Int. Cl[6]: H04L 29/06

22 Filed: 1/25/95

30 Priority data: 2/1/94 FR 9401091

43 Date of publication:
8/9/95 Bulletin 95/32

84 Designated contracting states:
AT BE CH DE DK ES FR GB GR
IE IT LI LU MC ML PT SE

72 Inventor: Basset, Jean-Claude
84, rue Vergniaud
F-75013 Paris (FR)

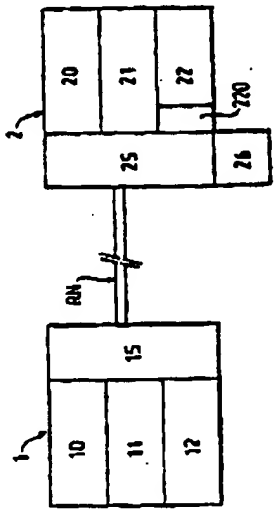
74 Attorney or Agent: Plaçais, Jean-Yves
Cabinet Netter,
40, rue Vignon
F-75009 Paris (FR)

71 Applicant: DASSAULT AUTOMATISMES ET
ET TELECOMMUNICATIONS
9, rue Elsa Trioist
Z.I. Les Gatines,
B.P. 13
F-78373 Plaisir Cédex (FR)

54 **Communication over digital network with antivirus protection**

57 A station (1) transmits file data through a communication interface (15) and using a given protocol, towards the communication interface (25) of a receiving station (2). This receiving station (2) temporarily stores the data sent by the transmitting station (1) in specific memory (26), which submits them to an antivirus scanner module (220) before it transforms them into data usable by a processing unit (22), if the virus scan is negative.

FIG.2



[stamped: EP 0 666 671 A1]

The invention concerns wide area computer communication networks, particularly public ones.

Generally these networks transmit information or raw data. However, there is now a tendency to use them also to send files, which are a set of organized data.

In France, for example, the company FRANCE TÉLÉCOM has now standardized a file transfer protocol called STUDEL, and developed a corresponding file transfer application named TÉLÉDISQUETTE. This file transfer system uses the integrated services digital network (ISDN) and is marketed under the trade name NUMÉRIS.

The change over to transferring files which are directly usable in a microcomputer presents numerous advantages. Firstly, the mode of connecting users can be standardized, as can the software used for the transfer, which allows multi-platform [manufacturer] and multi-user compatibility. In addition, this system can be combined with a directory listing the receivers of this service, and can also offer automatic broadcasting functions. In short, a technique for transferring files by public network can be envisaged which possesses almost the same characteristics of ease-of-use as the current voice telephony.

However, such a system is vulnerable to the transmission of files containing an intruding and/or harmful agent such as a computer virus.

The present invention provides a solution to this problem.

It is based on a computer communication device which includes:

- at least one transmitting station equipped with a processing unit with temporary memory and mass memory, and a communication interface,
- at least one receiving station equipped with a processing unit with temporary memory, mass memory, and a communication interface,
- with both communication interfaces able to communicate across a public digital network, and both stations equipped with communications modules, respectively transmitting and receiving, conforming to a predetermined protocol suitable for file transfer.

According to the present invention, the receiving station contains specific memory which is generally unable to exchange data with its processing unit, except possibly for the receiver communication module, as well as an antivirus scanning module; the communication module stores the incoming file data in said specific mass memory; it passes them to the antivirus

scanner module before changing them into a usable file and making them generally accessible to the processing unit.

The antivirus scanning module can operate using file data received serially, while receiving. It can also operate on grouped file data, for example in a temporary file, before changing them into a usable file.

Of course, the roles of the transmitters and receivers are not fixed as indicated, and one can well imagine a transmitter also being a receiver, and vice versa.

More generally, the communications module of the transmitter can be equipped with antivirus protection such as that of a receiver.

A special mode can also be provided where the receiving module is able to substitute for the current antivirus scanning module an updated version of [that module] received from the transmitter, after testing the updated version with the version previously available.

Other characteristics and advantages of the invention will appear upon examination of the detailed description which follows and the attached figures, in which:

- figure 1 is a general illustration of transmitters and receivers interconnected by the public digital network;
- figure 2 is a schematic diagram showing only one transmitting station and one receiving station; and
- figures 3 and 4 are two partial diagrams detailing two embodiments of the present invention.

In figure 1, the label RN indicates a wide area, or public, digital network, such as the integrated services digital network known in France under the name "Numéris".

Transmitters SV1 and SV2, as well as receivers AB1 to AB4, can be connected to this network

The transmitting and receiving stations are, for example (non-restrictive), equipped in the manner of microcomputer systems.

Thus in Figure 2, the transmitter 1 consists of one processing unit 10 with temporary memory 11 and mass memory 12, as well as a communication interface 15, which can also contain electronic functions.

In the same manner, the receiving station 2 is equipped with a processing unit 20, temporary memory 21, mass memory 22, and a communication interface 25, the latter also possibly having integrated functions.

The two communication interfaces 15 and 25 are able to communicate across the digital network RN. The two stations are equipped with communications modules which are transmitting and receiving respectively, operating by example in conformance with the TÉLÉDISQUETTE transfer application, which allows file transfers and is based on the aforementioned standardized protocol STUDEL (also designated EUROFILE TRANSFER in the ETS standard from the EUROPEAN TELECOMMUNICATION STANDARD INSTITUTES).

A file transfer system generally has its own security mechanism, using access codes and authentication, for example, which requires joint agreement by the transmitter and the receiver.

However, opening such a service to all users implies that certain files could be sent without prior agreement from those involved, therefore without setting in motion the security mechanism internal to the file transfer system.

Thus a transferred file can be infected with a computer virus.

A computer virus is a sequence of data introduced into a software program and/or a file, and which can initiate actions harmful to the normal operation of the computer system containing it. It is known that a virus can be active, passive, or triggered, for example.

Of the antivirus protection technology known, we can ignore those which only detect the presence of a virus by noting its effects after they are produced. This detection of viruses by their noted effects is hardly applicable here: in principle it signifies that the virus was already able to infect numerous local files.

The most effective techniques detect computer viruses by their structure, and/or as soon as the viruses begin to act. If necessary, they correct the effects of the detected virus as much as is possible. This is what is called an "antivirus scanner" here.

However, viruses vary greatly and their creators are imaginative. New viruses appear regularly. It is desirable to perform regular updates to the antivirus scanning tool, in order to include new virus structures recently uncovered.

The standard virus scanning application requires numerous manual steps to be performed each time new files are received, whether on diskette or in some other manner. Moreover, it is preferable to place questionable files on diskette for verification.

In the present invention, the receiving station 2 contains a part of specific memory represented here in 26 next to the communication interface 25.

By hardware or software means, this specific memory 26 is eligible to be generally unable to exchange data with its processing unit 20, except possibly for the receiver communication module 25.

A means of accomplishing this consists of equipping the computer system with a second independent hard drive, accessible only to the communication interface 25, which then contains appropriate means for managing such a hard drive.

Another method in operating systems with file read and write access privileges, consists of making part of the mass memory 22 reserved for reads and writes by the communication module 25, at least when the latter is in operation.

A third method could consist of reserving file access for the communication interface 25 only, being careful to give these files properties such that they cannot be used by the processing unit, particularly as program files, which are also called executable files.

An antivirus scanner module 220 is placed either in the mass memory 22 or in the part of the additional memory 26 when the latter has sufficient room.

The communication module 25 stores the entire incoming file data in the mass memory portion 26, and submits it to the antivirus scanner module before transforming it into a usable file, and then in addition making the file generally accessible (meaning without reservation) to the processing unit 20.

As was indicated above, the memory 26 can be mass memory directly accessible to the communication interface 25. In figure 3A, this memory is illustrated in 261 in the form of a high-capacity register or memory for which addressing and reads are restricted to the antivirus module illustrated in 220A. The latter module only authorizes access to the received data (shown in the diagram by closing switch 28A) when it is able to ensure that the data received are devoid of any known virus.

In other words, the antivirus module 220A operates here on the file data received serially, while receiving.

An expert in the field will know from figure 3A how to implement a device with several sections in memory 261, allowing serial reception of data while checking them and also allowing them to exit serially by appropriately closing the switch 28A.

The antivirus module preferably (at least for large files) acts on data grouped in files. This is what is illustrated in figure 3B.

The mass memory 26 is then an additional hard drive 262, where one can store all data received from the transmitter, in the form of temporary files (indicated by "TMP") for example.

The check can then be performed after the file has been completely received, by the antivirus module illustrated here in 220B, which as before has access to addressing and reading the hard drive 262.

When the check is complete, the module 220B authorizes access, shown in the diagram by closing the switch 28B, to the primary mass memory 22B in receiving station 2, where the received file can, for example, be transformed into an executable file (noted by the label "EXE").

In a manner which is completely unknown to the transmitting module, the receiving module can thus verify that all the received files are devoid of any virus.

Of course, a check of the same type can be performed at the transmitting module.

In addition, one can use exactly the same organization in the transmitting module as in the receiving module if need be, particularly if the transmitter can also play the role of receiver for other transmitters.

For the reasons already indicated, the antivirus protection module 220 may have to be modified in order to incorporate new versions of viruses recently discovered.

An interesting embodiment of the invention consists of sending the antivirus modules from a transmitter.

In this case, the receiving module will receive a special order representing a special mode of operation. It receives the new or updated antivirus protection module as it would any other file. After verification of it by the antivirus module it currently has, it will be able to replace the current one by the new antivirus module, at least if the check was negative.

Of course, the present invention is not limited to the implementation described here. It covers any variation which an expert in the field could develop, particularly within the framework of the following claims.

For reasons which are readily understood, the present description does not enter into detailing the known structures of computer viruses, nor the different variants of the invention which can result.

This being so, the phrase "computer virus" is to be understood in its widest sense, covering any intruding or deliberately added agent which can have a harmful or negative effect, even mild, on a computer system. It is known that the harmful action can simply consist of uselessly occupying space in random access memory or in mass memory. Therefore the invention can apply not only to the so-called "viruses" which infect an information system by propagating and multiplying in parallel with their harmful activities (just as biological viruses do), but also their software variants such as the Trojan Horse, bombs, and worms.

Such variants exist concerning the network used:

- the service described above (ISDN/DNS-Numéris) operates in "circuit" mode, meaning it links the two stations by simulating a direct connection between them;
- the invention can also apply to transmission methods called "[illegible]ram" or with packets (standard X25) in which the different groups or packets of data can take different routes. The amount of memory used to group the data is adjusted accordingly.

Variants also exist concerning the role of the stations:

- in "server" mode, a limited number of stations exist (the servers) which are dedicated to sending files to ordinary stations (subscribers) within point-to-point connections via a public or wide area network, which is suitable for organizations with centralized service, for example for remote distribution, uploading and downloading, or remote maintenance of software.
- in another mode ("station"), only transmitting or receiving stations, or more frequently transmitting/receiving stations, are considered. These are, for example, the subscribers for the server mode, which communicate directly with each other to exchange files.

Claims

1. A computer communication device comprising:

   - at least one transmitting station (1) equipped with one processing unit (10) with temporary memory (11), mass memory (12), and a communication interface (15).

   - at least one receiving station (2) equipped with one processing unit (20) with temporary memory (21), mass memory (22), and a communication interface (25),

   - with the two communication interfaces (15, 25) able to communicate across a digital network (RN), and the two stations equipped with transmitting and receiving communication modules respectively, in conformance with a predetermined protocol suitable for file transfer,

   wherein the receiving station (2) contains a part of specific memory (26) eligible to be generally unable to exchange data with its processing unit, except for the receiving communication module, as well as an antivirus scanning module (220), wherein the communication module (25) stores the incoming file data in said part of mass memory (26), and wherein it submits them to the antivirus scanning module (220) before transforming them into a usable file and making them generally accessible to the processing unit.

2. A device according to claim 1, wherein the antivirus module (220A) operates on file data received serially, while receiving (261).

3. A device according to one of claims 1 and 2, wherein the antivirus module (220B) operates on the group of file data (262) before they are transformed into a usable file (22B).

4. A device according to one of the above claims, wherein the communication module (15) of the transmitter is equipped with a means of antivirus protection such as that of a receiver.

5. A device according to one of the above claims, wherein a special mode allows the receiving module to substitute for the current antivirus module an updated version of it, received from the sender, after checking the updated version with the prior version.

6. A device according to one of the prior claims, wherein said part of special memory (26) is part of the mass memory, or is additional mass memory (22B).

7. A device according to one of the prior claims, wherein the communication protocol is a standard protocol for public use.

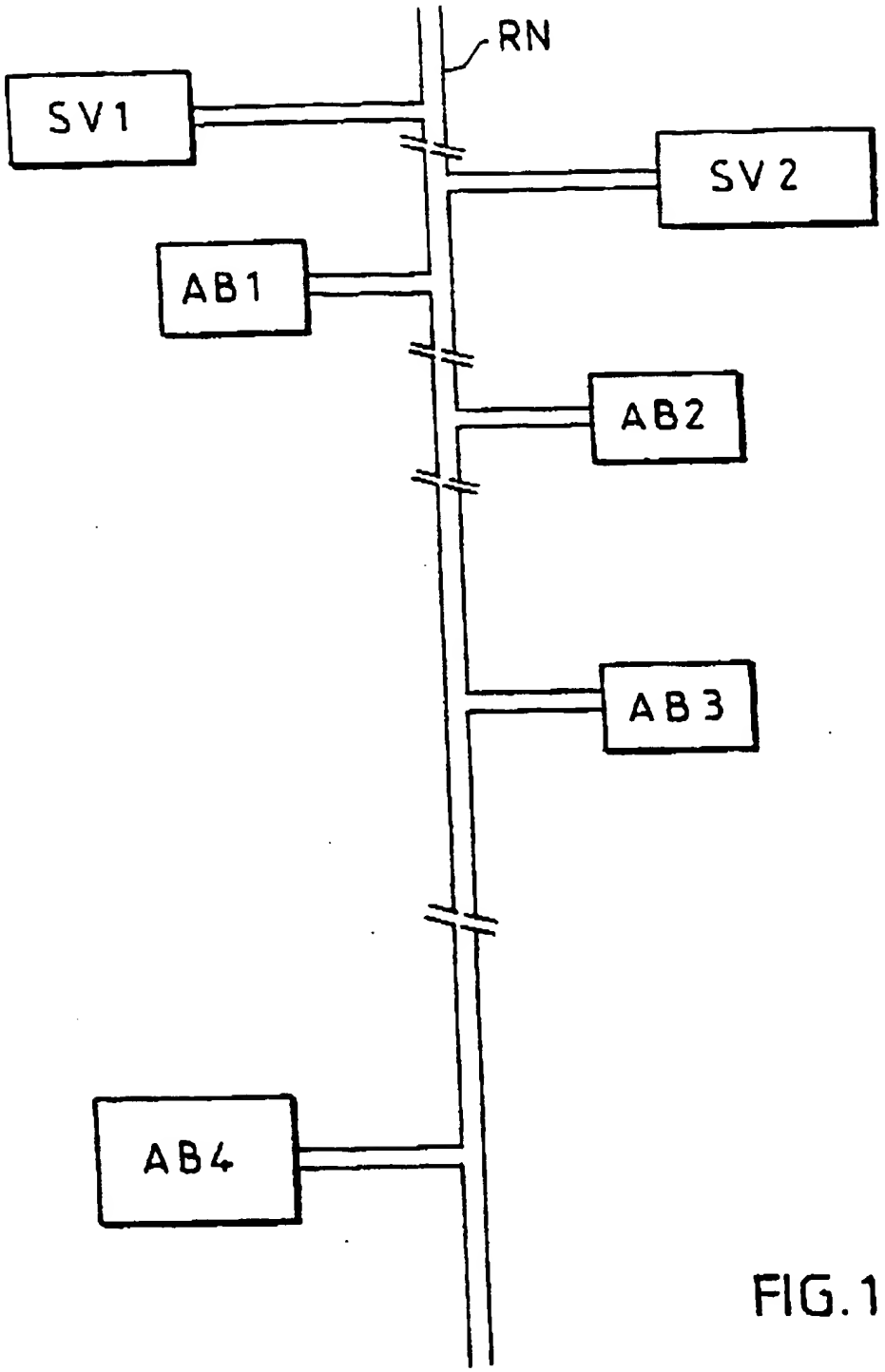


FIG.1

FIG. 2

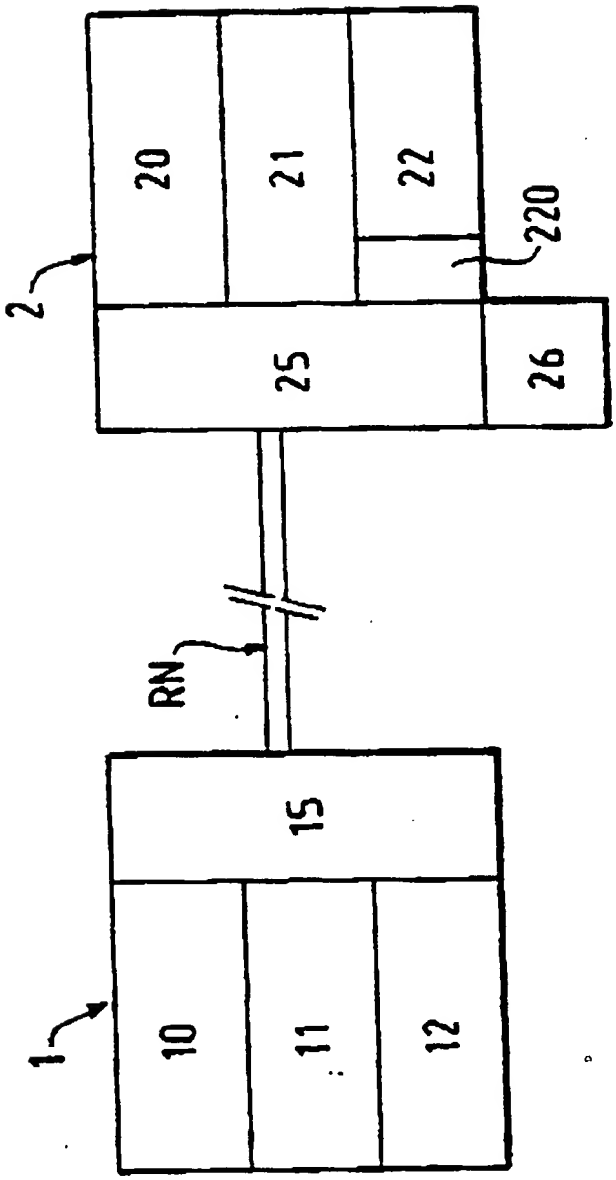


FIG. 3B

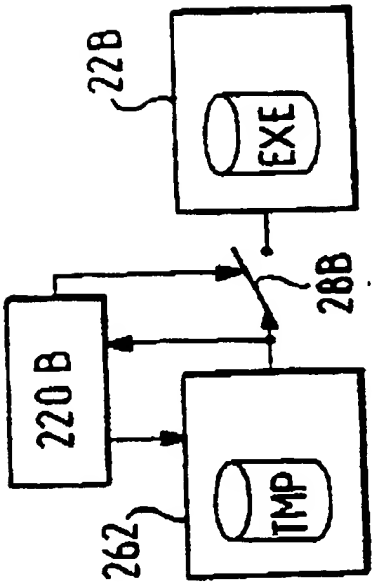


FIG. 3A